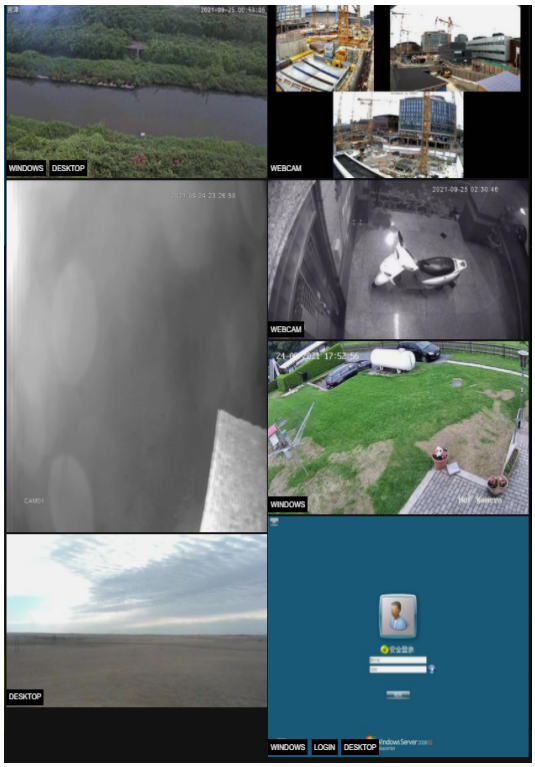
Lab 5

Exploring Shodan



Estimated time to complete: 20 Min

WHAT YOU WILL LEARN

Shodan is a search engine for Internet-connected devices. Search for open ports or abuse default passwords to discover everything from web cams, power plants, cell phones, refrigerators, and Minecraft servers.

Let's go exploring and see what we can find!

WHY IT'S IMPORTANT

Explore and understand the dangers that come with a lack of security with devices connected to the open network

Understand the basics of port scanning across the entire internet and how attackers can find your device even without it being connected to a domain name

SKILLS GAINED

- Port scanning
- Open Source Intelligence
- Understanding of "Open Internet"
- How to view open devices

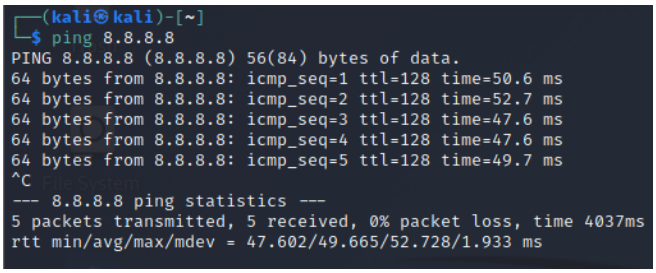
REQUIRED HARDWARE

- Raspberry Pi
- Internet connection

DISCLAIMER: THIS LAB WILL YOU SHOW YOU HOW TO VIEW THESE PUBLIC DEVICES. HOWEVER, TRYING TO ACCESS OR CONTROL THESE DEVICES IS ILLEGAL. USING SHODAN IS LEGAL, ACCESSING SOMEONE ELSE'S DEVICE IS NOT! DO NOT ATTEMPT TO USE OR MODIFY THE DEVICES FOUND.

INTRODUCTION TO SHODAN

Shodan is a search engine for cyber security individuals. Unlike Google, Shodan allows its users to search for devices that are open to the public internet and filter those results based on the users wants. It achieves this through the port scanning of every device broadcasting to the open internet. We can find devices in Shodan based on their IP address, an IP address is like the mailing address of a computer or any internet connected device. We can send information to a device and receive information from a device by talking to its IP. Every device on Shodan will have open ports, a port is basically a note that is connected to the IP address to tell the device where your message should go once it is received. There are ports for emails, webpages, cameras, and remote connections. The most common ports used can be found here: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers. The type of port you find is going to determine what you are going to see! Lastly, let's go over the idea of pings. A ping request basically asks the device if it's alive. If it is alive it will respond, there is a time attached to these responses, this is how long it took for the device to respond. If the device is dead or purposely not responding to pings, the request will time out, this is how Shodan finds working devices to probe for open ports.



Successful ping request

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.200
PING 192.168.1.200 (192.168.1.200) 56(84) bytes of data.
From 192.168.1.50 icmp_seq=3 Destination Host Unreachable
^C
--- 192.168.1.200 ping statistics ---
115 packets transmitted, 0 received, +1 errors, 100% packet loss, time 116726ms
```

Failed ping request

USING FILTERS

Shodan uses tools known as filters. These filters allow you to narrow down your results based on what you are trying to find. Instead of searching through millions of devices, you can choose to search just for devices that meet your criteria. This could include searching for devices in your town, those who are running services on a specific port, or even showing just webcams! This can be very useful as if you are trying to find multiple servers that are running a program on port 754 you can have all your results neatly organized without ever having to ping the device yourself. The full list of filters can be found here: https://www.shodan.io/search/filters with a cheatsheet of the most common filters below.

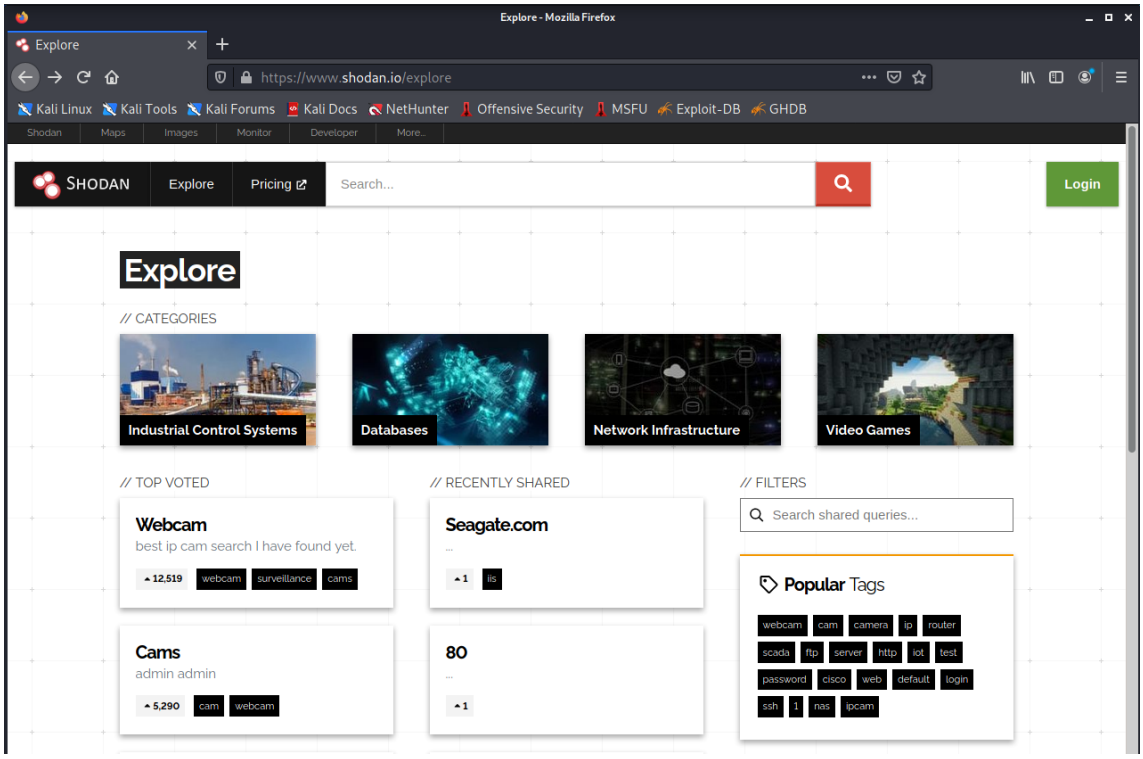
Filters Cheat Sheet

Shodan currently crawls nearly 1,500 ports across the Internet. Here are a few of the most commonly-used search filters to get started.

Filter Name	Description	Example
city	Name of the city	Devices in San Diego
country	2-letter Country code	Open ports in the United States
http.title	Title of the website	"Hacked" Websites
net	Network range or IP in CIDR notation	Services in the range of 8.8.0.0 to 8.8.255.255
org	Name of the organization that owns the IP space	Devices at Google
port	Port number for the service that is running	SSH servers
product	Name of the software that is powering the service	Samsung Smart TVs
screenshot.label	Label that describes the content of the image	Screenshots of Industrial Control Systems
state	U.S. State	Devices in Texas

HOW TO USE SHODAN

In order to access Shodan, first go to https://www.shodan.io/explore in order to view the homepage of the site. Here you can see all of the most popular categories that people use to view devices. On the top search bar you can manually enter a search item such as an ip or filter combo. Located on the column to the right of the screen are popular tags that can be used to quickly search and find devices.



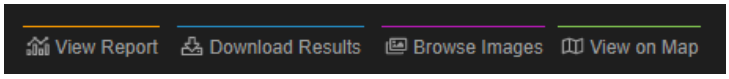
However, before we can start searching the internet for all it has to offer, we have to make an account. We can create one at: https://account.shodan.io/login . Once we have made an account, we can return to the explore page and start searching!

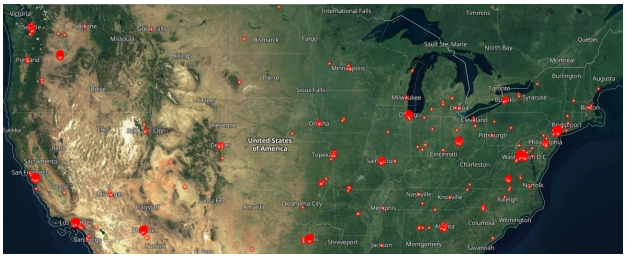
VIEWING REMOTE DESKTOP

Remote desktop is a tool that allows you to connect to your computer over the internet. This is very useful for accessing your devices from a different location but if left unsecure your

machine can be found and accessed by anyone who scans your IP address. You can search for this by using the filter "***port:3389 has_screenshot:true***". Port 3389 is the port dedicated to remote desktop, you can also filter by country adding "***country:US***" to your filter (use the 2 digit country code). You should find a ton of desktops with this enabled and you can see the users who have accounts on these machines.

On the top bar of the search results screen, you can click "***Browse Images***" to see a screen view of all the vulnerable devices, or you can click "***View on Map***" to see where these machines are physically located, you can move and zoom the map, then click the pin to see information about that device.



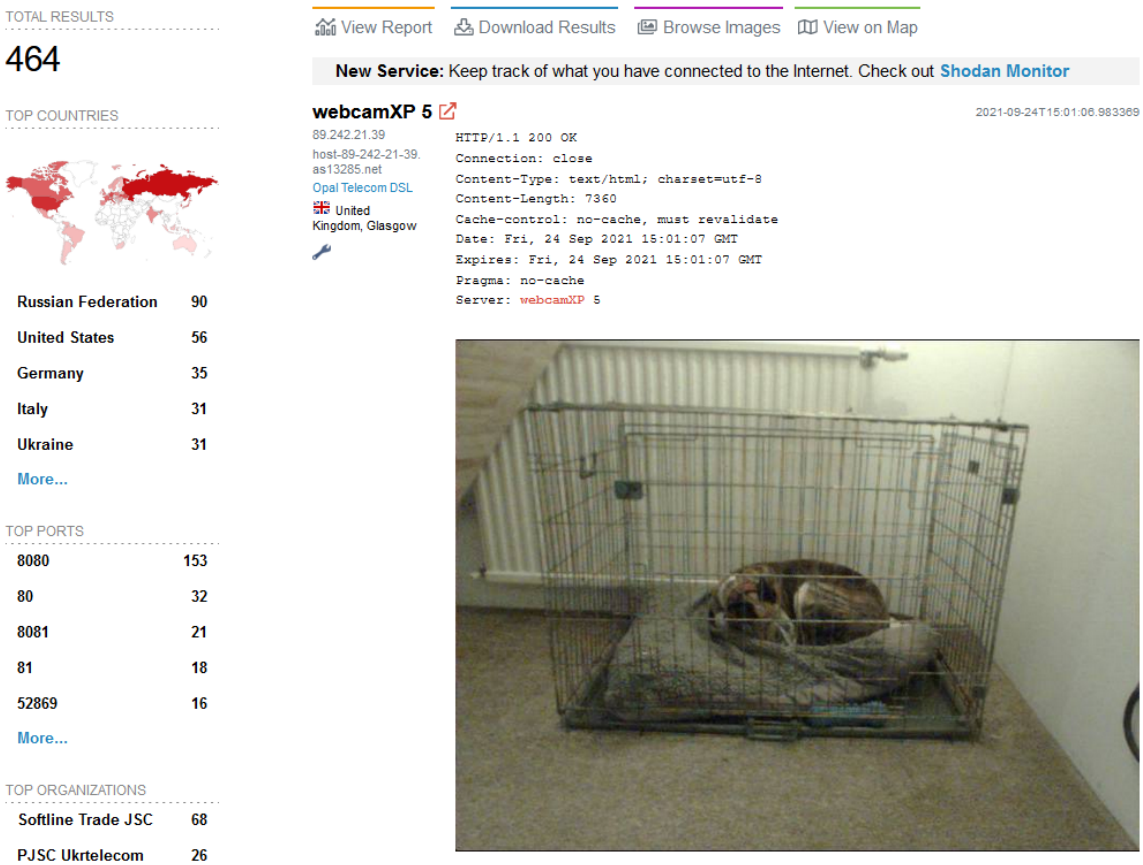


VIEWING WEBCAMS

One of the most controversial uses of Shodan is the ability to view others webcams. We are able to achieve this by searching different webcam services available on the open internet.

For this demonstration we are going to be viewing devices that are currently running the service, “webcamxp”. WebcamXP is an outdated webcam and network camera software for legacy Windows devices that allows its users to view the webcam remotely. Similar to other aspects in the technology industry, even though it's outdated and insecure, people still use the service because of compatibility issues or more commonly, laziness.

We can view these devices by going to the search bar on the explore page and using the keyword “***webcamxp***” hit enter. Once we’ve done this we can start to scroll through the different devices running this service (Seen Below). Spend a few minutes searching through these devices and formulate what security issues could come from this.



webcamXP 5

2021-09-24T14:52:01.357034

95.248.81.168
host-95-248-81-168.retail.telecomitalia.it
Telecom Italia S.p.A.
Italy, Florence

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7589
Cache-control: no-cache, must revalidate
Date: Fri, 24 Sep 2021 14:51:50 GMT
Expires: Fri, 24 Sep 2021 14:51:50 GMT
Pragma: no-cache
Server: webcamXP 5
```

93.90.222.25

2021-09-24T14:34:55.009178

Softline Trade JSC
Russian Federation, Moscow

honeypot

```
HTTP/1.1 200 OK
Server: 360 web server, 792/71644  HTTP Server version 2.0 - TELDAT S.A., A10WS/1.00,
```

webcamXP 5

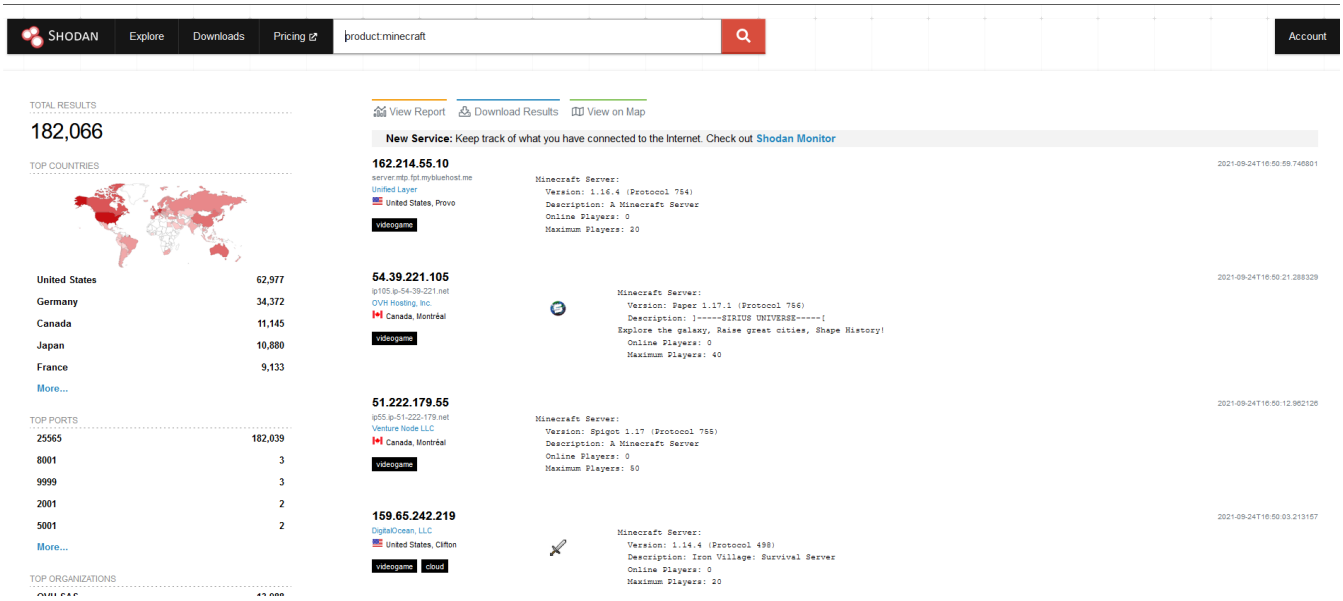
2021-09-24T14:23:14.422188

64.118.101.86
6411810186.static.sti.net
Sierra Tel Internet
United States, Oakhurst

```
HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 7413
Cache-control: no-cache, must revalidate
Date: Fri, 24 Sep 2021 14:23:09 GMT
Expires: Fri, 24 Sep 2021 14:23:09 GMT
Pragma: no-cache
Server: webcamXP 5
```

VIEWING GAME SERVERS

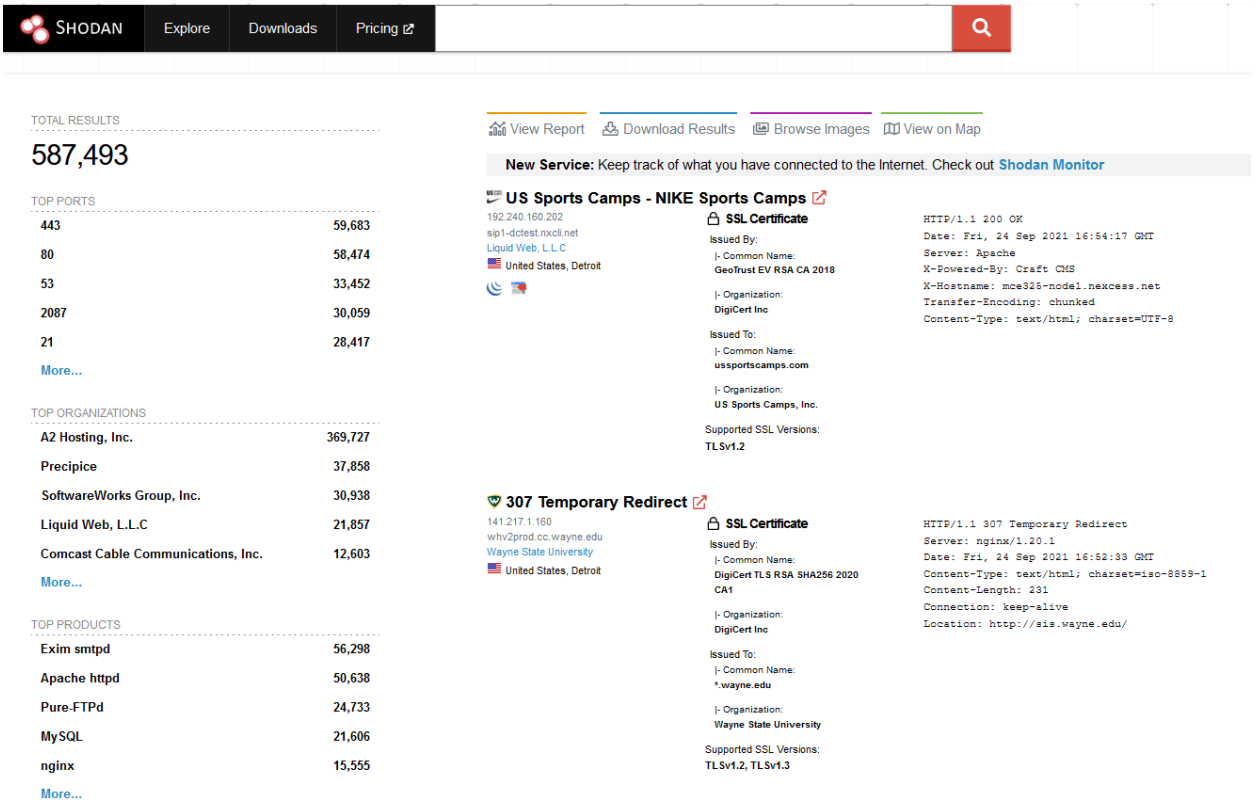
You can also use Shodan to look at video game servers! Click on the explore tab and click on the Video Games category. You'll see several games such as Minecraft, Counter Strike, and Rust. In this lab, we'll be taking a look at Minecraft servers. ***Click on Video Games, then Explore Minecraft*** to see how many servers you can find on Shodan. You will be able to see the version, a description of the server, the number of online players, and the maximum number of players. You can also see the server IP address as well as the location where the server is being hosted. Click around on the IP addresses to see a more detailed view of the servers. You can see what ports are being used, the domains being used to host the servers, and in some cases it will show potential vulnerabilities. Take a few minutes to click around on different servers and see if you can find any with vulnerabilities that Shodan suspects.



EXERCISES:

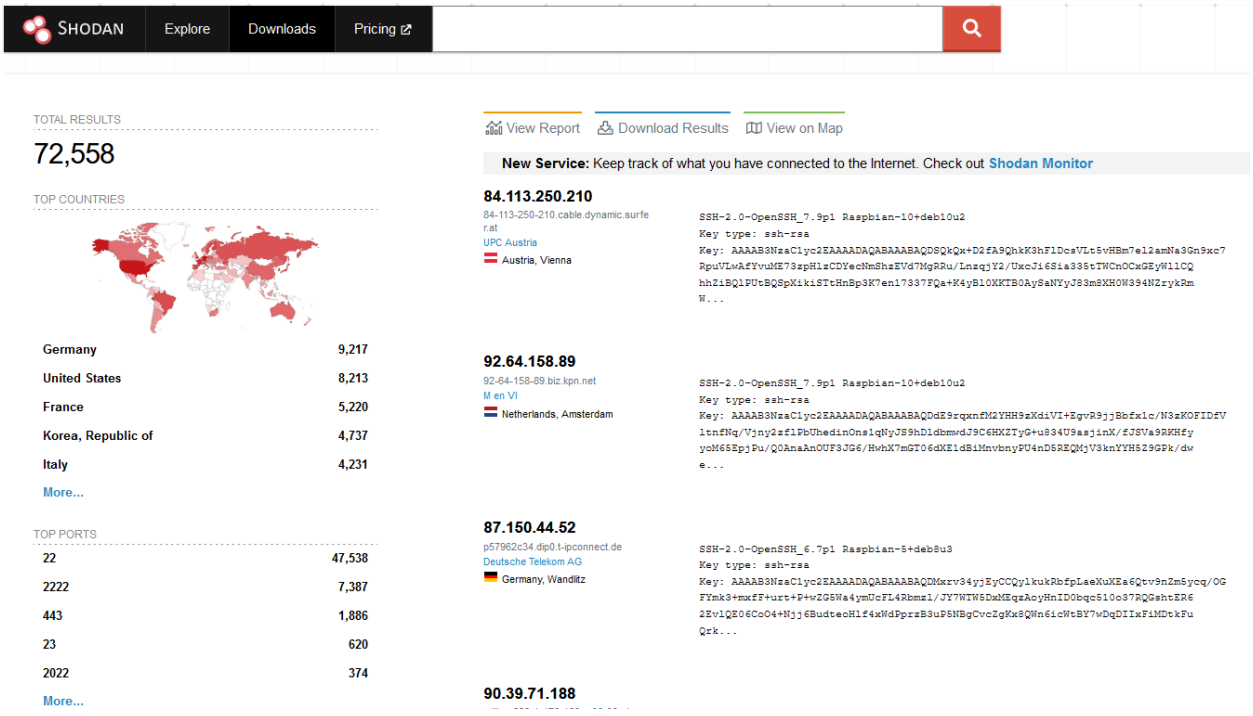
1: Location Discovery:

For this exercise, try finding open devices within your hometown! Shodan's filters allow you to discover devices in an area. Below is a list of devices in Detroit, MI



2: Find legacy hardware based on operating systems:

Oftentimes people are lazy or don't have the ability to upgrade old computer systems that are highly insecure. In this exercise, try to find devices that are still running Windows XP which ended security support on January 14, 2020! Below is a list of computers running Raspbian


SHODAN
Explore
Downloads
Pricing
TOTAL RESULTS
72,558
TOP COUNTRIES
Germany 9,217
United States 8,213
France 5,220
Korea, Republic of 4,737
Italy 4,231
More...
TOP PORTS
22 47,538
2222 7,387
443 1,886
23 620
2022 374
More...
View Report
Download Results
View on Map
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
84.113.250.210
84-113-250-210.cable.dynamic.surfer.at
UPC Austria
Austria, Vienna
SSH-2.0-OpenSSH_7.9p1 Raspbian-10+deb10u2
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDSQkQx+D2fA9QhkK3hF1DcsVLt5vHBm7el2amNa3Gn9xc7
RpuVLwAfYvuME73zpHlzCDYecNmShzEVd7MgRRu/LnzqjY2/UxcJi6Sia33StTWCnOCxGEyW1lCQ
hhZiBQ1PUtBQSpXikiSTtHnBp3K7en17337FQa+K4yBlOKKTBOAySaNYyJ83m8XH0W394NZrykRm
W...
92.64.158.89
92-64-158-89.biz.kpn.net
M en VI
Netherlands, Amsterdam
SSH-2.0-OpenSSH_7.9p1 Raspbian-10+deb10u2
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDdE9rqxnfM2YHH9zXdiVI+EgvR9jjBbfx1c/N3zK0FIDfV
ltnfNq/Vjny2zf1PbUhedinOns1qNyJS9hDldbmwdJ9C6HXZTyG+u834U9asjinX/fJSVa9RKHfy
yoM65EpjPu/Q0AnaAnOUF3JG6/HwhX7mGT06dXE1dBiMnvbnyFU4nD5REQMjV3knYYH5Z9GPk/dw
e...
87.150.44.52
p57962c34.dip0.t-ipconnect.de
Deutsche Telekom AG
Germany, Wandlitz
SSH-2.0-OpenSSH_6.7p1 Raspbian-5+deb8u3
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDMxrv34yjEyCCQylukukRbfpLaeKuKEs6Qtv9nZm5ycq/OG
FYmk3+mxfF+urt+P+wZG5Wa4ymUcFL4Rbmzl/JY7WW5DxMEqzAcyHnID0bqc510c37RQGshtER6
2Evl0E06CoO4+Njj6BudteoH1f4xWdPprzB3uP5NBgCvcZgKx8QWn6icWtBY7wDqDIIxFiMDtkFu
Qrk...
90.39.71.188

REVIEW

1: Web servers are hosted on what ports?

A) 89/314

B) 312/765

C) 80/443

D) 14/214

2: Default security settings are often enough to be secure on the internet (True/False)

3: Which isn't a filter on shodan?

A) city

B) webcam

C) jonstar

D) product:minecraft

4: Shodan is used *only* for hacking it has no purpose for securing your network (True/False)

5: Port scanning your network allows what?

A) See services that face the open internet

B) Detect malicious/unknown servers

C) Know your networks vulnerabilities

D) All of the above

6: Select the correct statement

A) Using Shodan is Illegal and accessing devices is legal

B) Using Shodan is legal and accessing devices is illegal

C) Using Shodan is Illegal and accessing devices is illegal

D) Using Shodan is legal and accessing devices is legal

Answers: 1:C 2:F 3:C 4:F 5:D 6:B